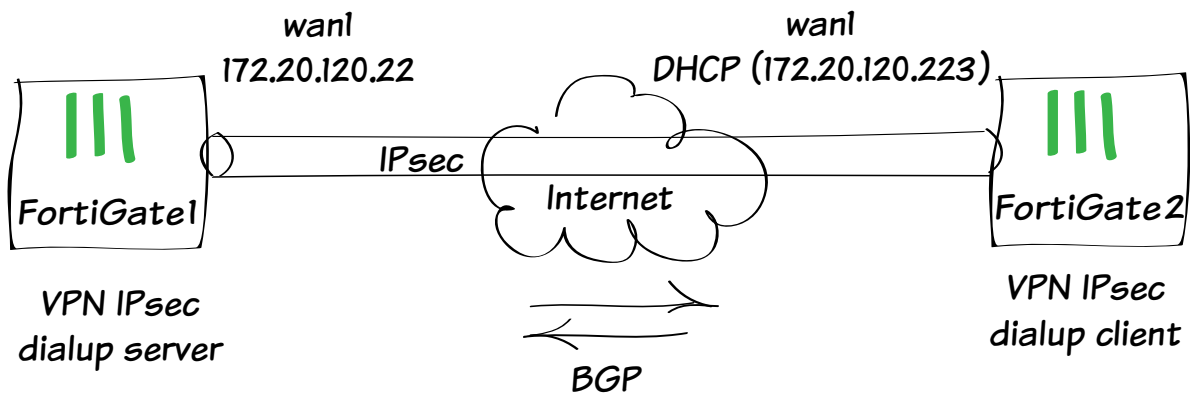


Setting up BGP over a dynamic IPsec VPN between two FortiGates

This example shows how to create a dynamic IPsec VPN tunnel and allowing BGP to establish through it.

1. Configuring IPsec in Fortigate1
2. Configuring IPsec in FortiGate2
3. Verifying tunnel is UP
4. Configuring BGP in FortiGate1
5. Configuring BGP in FortiGate2
6. Results



1. Configuring IPsec in FortiGate 1

Go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

Click **Next**.

1 VPN Setup > 2 Authentication > 3 Policy & Routing

Name: ike-bgp-fgt1

Template:

- Dialup - FortiClient (Windows, MacOS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set **Remote Gateway**, **Outgoing Interface** and **Pre-shared Key**.

Click **Next**.

✓ 1 VPN Setup > 2 Authentication > 3 Policy & Routing

ike-bgp-fgt1 : Site to Site - FortiGate

Remote Gateway: 172.20.120.223

Outgoing Interface: wan1 (Detected via routing lookup) [\[Change\]](#)

Authentication Method: ☒ Pre-shared Key ☐ Signature

Pre-shared Key:

☒ Hide Characters

< Back Next > Cancel

Set **Local Interface**, **Local** and **Remote Subnets**.

Click **Create**.

FortiGate then will create phase 1, phase 2, static route, local and remote address group, local to remote and remote to local security policies.

The screenshot shows the 'Policy & Routing' step of the VPN Setup Wizard. The wizard has three steps: VPN Setup (checked), Authentication (checked), and Policy & Routing (active). The title bar reads 'ike-bgp-fgt1 : Site to Site - FortiGate'. Below the title bar, there are three input fields: 'Local Interface' with a dropdown menu showing 'lan', 'Local Subnets' with a text box containing '192.168.1.0/24' and a help icon, and 'Remote Subnets' with a text box containing '10.10.1.0/24' and a help icon. At the bottom, there are three buttons: '< Back', 'Create', and 'Cancel'.

The screenshot shows the 'Policy & Routing' step of the VPN Setup Wizard after successful completion. The title bar reads 'ike-bgp-fgt1 : Site to Site - FortiGate'. Below the title bar, there is a green checkmark icon followed by the text 'The VPN has been set up successfully'. Below this, there is a section titled 'Summary of Created Objects' with a table listing the created objects:

Phase 1 Interface	<i>ike-bgp-fgt1</i>
Phase 2 Interfaces	<i>ike-bgp-fgt1</i>
Static Routes	<i>10.10.1.0/24</i>
Local Address Group	<i>ike-bgp-fgt1_local</i>
Remote Address Group	<i>ike-bgp-fgt1_remote</i>
Local to Remote Policy	<i>5</i>
Remote to Local Policy	<i>7</i>

At the bottom, there are two buttons: 'Add Another' and 'Show Tunnel List'.

2. Configuring IPsec in FortiGate 2

Go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.
Click **Next**.

1 VPN Setup

2 Authentication

3 Policy & Routing

Name

ike-bgp-fg2

Template

Dialup - FortiClient (Windows, Mac OS, Android)

Site to Site - FortiGate

Dialup - iOS (Native)

Dialup - Android (Native L2TP/IPsec)

Dialup - Cisco Firewall

Site to Site - Cisco

Custom VPN Tunnel (No Template)

Set **Remote Gateway, Outgoing Interface** and **Pre-shared Key**.
Click **Next**.

1 VPN Setup

2 Authentication

3 Policy & Routing

ike-bgp-fg2 : Site to Site - FortiGate

Remote Gateway

172.20.120.22

Outgoing Interface

wan1 (Detected via routing lookup) [\[Change\]](#)

Authentication Method

☒ Pre-shared Key

☐ Signature

Pre-shared Key

.....

☒ Hide Characters

< Back

Next >

Cancel

Set **Local Interface, Local** and **Remote Subnets**.
Click **Create**.

VPN Setup

Authentication

3 Policy & Routing

ike-bgp-fg2 : Site to Site - FortiGate

Local Interface

internal

Local Subnets

10.10.1.0/24

Remote Subnets

192.168.1.0/24

< Back

Create

Cancel

FortiGate then will create phase 1, phase 2, static route, local and remote address group, local to remote and remote to local security policies.

VPN Setup

Authentication

Policy & Routing

ike-bgp-fg2 : Site to Site - FortiGate

The VPN has been set up successfully

Summary of Created Objects

Phase 1 Interface

ike-bgp-fg2

Phase 2 Interfaces

ike-bgp-fg2

Static Routes

192.168.1.0/24

Local Address Group

ike-bgp-fg2_local

Remote Address Group

ike-bgp-fg2_remote

Local to Remote Policy

2

Remote to Local Policy

3

Add Another

Show Tunnel List

3. Verifying tunnel is UP

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is **UP**.

Name	Remote Gateway	Status	Uptime
ike-bgp-fgt1	172.20.120.223	Up	55 Minutes 56 seconds

4. Configuring BGP in FortiGate 1

Go to **System > Status** to look for **CLI Console** widget and type the following:

```
config router bgp
  set as 1
  set router-id 172.20.120.22
  config neighbor
    edit "172.20.120.223"
      set remote-as 2
    next
  end
  config redistribute "connected"
    set status enable
  end
  config redistribute "static"
    set status enable
  end
end
```

5. Configuring BGP in FortiGate 2

Go to **System > Status** to look for **CLI Console** widget and type the following:

```
config router bgp
  set as 2
  set router-id 172.20.120.223
  config neighbor
    edit "172.20.120.22"
      set remote-as 1
    next
  end
  config redistribute "connected"
    set status enable
  end
  config redistribute "static"
    set status enable
  end
end
```

6. Results

From FortiGate 1, Go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 2 were successfully advertised to FortiGate 1 via BGP.

Type	Network	Gateway	Interface	Up Time
Static	0.0.0.0/0	0.0.0.0	fext-wan1	
Static	0.0.0.0/0	25.52.81.253	fext-wan1	
Static	10.10.1.0/24	0.0.0.0	ike-bgp-fgt1	
BGP	10.10.80.0/24	172.20.120.223	wan1	0 00:31:21
Connected	25.52.81.0/24	0.0.0.0	fext-wan1	
Connected	169.254.1.1/32	0.0.0.0	ssl.root	
Connected	169.254.1.1/32	0.0.0.0	ssl.root	
Connected	172.20.120.0/24	0.0.0.0	wan1	
Connected	192.168.1.0/24	0.0.0.0	lan	
Connected	::1/128	::	root	

From FortiGate 2, Go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 1 were successfully advertised to FortiGate 2 via BGP.

Type	Network	Gateway	Interface	Up Time
Static	0.0.0.0/0	172.20.120.2	wan1	
Connected	10.10.1.0/24	0.0.0.0	internal	
Connected	10.10.80.0/24	0.0.0.0	wifi	
BGP	25.52.81.0/24	172.20.120.22	wan1	0 00:52:04
BGP	169.254.1.1/32	172.20.120.22	wan1	0 00:52:04
Connected	172.20.120.0/24	0.0.0.0	wan1	
Static	192.168.1.0/24	0.0.0.0	ike-bgp-fg2	
Connected	::1/128	::	root	